AU/ACSC/LARIOS/AY12

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

POSTURING U.S. AIR FORCE INTELLIGENCE TO BETTER SUPPORT OPERATIONS AGAINST CYBER THREATS

by

Erwin A. Larios, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lt Col Robert C. Hume

Maxwell Air Force Base, Alabama

14 December 2011

CONTENTS

Disclaimer	ii
Abstract	iii
Section 1: Introduction	1
Section 2: U.S. Intelligence Community, DOD and Air Force	5
Section 3: Cyber Doctrine	10
Section 4: Intelligence Cyber Training	13
Section 5: Recommendations	17
Section 6: Conclusion	19
End Notes	20
Bibliography	22

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

The United States Air Force, like others within the national Intelligence Community (IC), does not provide adequate Intel support to cyberspace operations due to the unique complexity of cyber. Technology-based threats are so rampant that cyber recently emerged as a war-fighting domain—indicating its importance to decision makers. Although the DOD established Cyber Command, which leads the Defense Department cyber mission, Air Force Intel has made slow progress in embracing cyberspace challenges and posturing itself to provide support.

This paper outlines steps that must occur for the Air Force to provide timely and accurate intelligence support to cyberspace operations since the Air Force is not responding quickly enough to these threats. It describes the cyber domain, its importance, and the necessary mindset change to support cyberspace operations. Additionally, a cadre of cyber-savvy intelligence professionals should be created; otherwise significant progress will not come to fruition.

The discussion begins with a brief examination of the post-9/11 restructuring of the national IC for relevant historical data. This is followed by a look at the current mindset involving cyberspace operations, newly developed cyber doctrine, and necessary intelligence training. The paper concludes with recommendations that the Air Force might use to remedy the situation.

Introduction

Following the end of the Cold War, the United States surfaced as the premier global leader. In fact, it has enjoyed an unrivaled status since the demise of the former Soviet Union. However, despite the absence of a traditional competitor, multiple state and non-state actors continuously threaten the U.S. [1] As a result, there is a constant need to identify and monitor potential threats.

Senior decision makers within the U.S. government are concerned with maintaining national security and protecting U.S. interests abroad. They depend on the U.S. Intelligence Community (IC) to achieve this goal. In fact, our government leaders have made the collection, processing, assessment and dissemination of sensitive information regarding credible threats a top priority. [2]

The IC is composed of 17 leading intelligence organizations and agencies—all of which are considered to be experts in their respective fields—and are grouped into four categories: national intelligence organizations, Department of Defense intelligence organizations, military service intelligence organizations, and civilian intelligence organizations. [3] It is certainly not a simple structure since it revolves around the demands of the United States government for specific, sensitive information. Given this complexity, it is no surprise that the IC has had to overcome challenges—particularly as it morphs to address threats post-9/11 including cyber threats.

In 2001, in what amounted to a series of coordinated attacks in several locations throughout the United States involving the World Trade Center and the Pentagon, terrorists successfully executed heinous acts on U.S. soil using commercial aircraft. [4] It was simply inconceivable that the network of intelligence organizations established to detect and report credible threats had failed our national leadership and the American people. It soon became apparent that changes were going to be made if the system is to function as designed.

The 9/11 Commission Report identified information sharing as a major issue that required immediate resolve. [5] That is, there was a finding identified that IC members failed to properly coordinate intelligence. As a result, there was a concerted effort to address this issue.

In a similar fashion, cyber threats provide an equally important reason for change in today's information environment. That is, there are unique problems associated with the nature of cyberspace and the threats that exist in this domain. Therefore, one may reasonably state that a change in mindset is required since failing to do so may result in another 9/11-level catastrophic event. As opposed to individual airliners aimed at a handful of physical targets, the next major attack could occur within cyberspace and affect multiple independent entities within the U.S.

In 2007, organized crime groups attacked major Estonian government agencies and financial institutions—both of which were heavily reliant on the Internet. [6] This means the cyber domain may be utilized to negatively affect a substantial percentage of the government, the private sector, and the general populace at the same time. The Estonia example demonstrates the gravity cyber threats pose to our national security and outlines the need to defend against them.

The U.S. is making slow progress in this area. This is particularly the case when compared to the People's Republic of China (PRC), which is generally recognized as being a universal frontrunner in the cyberspace domain. [7] There does not seem to be a sense of urgency in the U.S. Air Force with regard to ensuring intelligence supports cyberspace to an adequate level. This may be due to the complexity of this domain, which basically means there must be a mental adjustment of sorts to greatly increase support geared towards negating potential cyber threats.

This paper focuses on intelligence efforts within the Department of Defense—specifically the U.S. Air Force. Although the 24th Air Force leads the service in spearheading assistance to the recently established U.S. Cyber Command (USCYBERCOM), there is more work required from

an Intel perspective. In fact, one of the major points considered is the inability of Air Force intelligence to properly support cyberspace operations at the present time.

The argument is made that the ubiquity of the cyber domain is the main culprit. That is to say, cyberspace is much different than the traditional domains of air, land, sea and space. This innate exclusivity demands an unusual way of thinking, which essentially accounts for this disconnect since most intelligence personnel tend to only fully comprehend the physical domains. They are essentially still learning the basic fundamentals of this man-made realm.

Another point of discussion involves cyber doctrine and reference documents. With the establishment of cyber as a domain, there have been numerous publications that have come to light that address cyberspace operations. Although this represents an improvement in and of itself, since these publications have come to exist within the last few years, progress in this area has been relatively sluggish. In addition, much of the information contained therein is very general in nature and surely lacks the specificity that may be of use in challenging cyber threats.

There is also a critical requirement for cyberspace training initiatives in the intelligence field. For the most part (excluding those few Air Force Intel analysts embedded in such organizations as the National Security Agency, NSA, or U.S. Cyber Command), intelligence personnel generally lack in-depth training in supporting operators within the cyber domain. In fact, while the Air Force grapples with obtaining a handle on cyber threats, it would not be an exaggeration to indicate that many are learning “on the job” in the absence of formal training programs.

This is a phenomenon recognized by senior Air Force intelligence leaders. As this document will discuss, there are efforts underway to assist in developing cyber-savvy Intel professionals. However, while there are serious efforts aimed at correcting this deficiency, it is certainly not an easy task to handle and is making slow progress at the present time.

In summary, changes to the Intelligence Community have been made in the spirit of adapting to emerging threats in a post-Cold War (and certainly post 9/11) era. However, there is a crucial requirement to improve intelligence support to cyberspace operations to prevent a potential "cyber 9/11" event. These include such issues as changing the mindset of senior leadership and Intel professionals, creating and understanding cyber doctrine and publications, as well as growing a cadre of intelligence personnel that comprehend basic cyber principles in order to provide tailored support to cyberspace operations. In the end, there should be a top-down holistic approach to cyberspace that must include the training of intelligence personnel to ensure timely and accurate information is afforded to senior decision makers and operators alike. There is no better way to affect change and correct this dilemma.

The U.S. Intelligence Community, DOD and Air Force

The National Security Act of 1947 began what we know today as the Intelligence Community with the creation of the Central Intelligence Agency (CIA). [8] Having evolved since then, the IC is defined as a "federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States." [9] However, there are only a few organizations that support cyberspace efforts; two of these are NSA and USCYBERCOM.

This multi-member system employs numerous methods of obtaining intelligence to keep decision makers informed of domestic and foreign threats. Collection techniques include—but are certainly not limited to—Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), Geo-spatial Intelligence (GEOINT), and Human Intelligence (HUMINT) to name just a few. While they vary in focus, each of these disciplines compliments the other in supporting senior leaders and operators during peace and war. In short, Intel has different ways to provide the critical data needed to make tough decisions at the strategic, operational and tactical levels of warfare.

The IC is not perfect. As former NSA Director and retired Army Lieutenant General William Odom once stated "…it had embarrassing failures that should not be tolerated… however, it has performed impressively, at times accomplishing remarkable feats." [10] There is an implication in this quote that the IC may have prevented some of its humiliating past failures, such as 9/11. Therefore, it follows that the identification of shortfalls (including the need for better overall intelligence support to cyber operations) should be taken seriously and acted upon quickly in an effort to avoid what seems to be another pending "embarrassing failure" by Intel collectively.

NSA makes up the bulb of the nation's SIGINT capability, which includes surveillance of cyber networks. It analyzes and exploits changing technology in support of national-level

leaders and tactical level military forces.[11] Due to the extensive information it collects using sensitive methods, it is a key player.

USCYBERCOM, established in May 2010 under the DOD, is slowly becoming a major player in the cyberspace realm. A sub-unified command under United States Strategic Command (USSTRATCOM), the USCYBERCOM commander is dual-hatted as the director of NSA as well. The rationale behind this is the commander/director will have sufficient flexibility in leveraging different U.S. Code authorities while addressing perceived cyber threats. That is, aligning different, but required, U.S. Code authorities under one individual ensures there is a collective effort between USCYBERCOM and NSA aimed at cyberspace operations.

USCYBERCOM was created as a method to unify Department of Defense efforts in cyberspace. Specifically, it will "direct the operations and defense of specified DOD information networks…conduct full-spectrum military cyberspace operations in order to enable actions in all domains… (and) ensure US/allied freedom of action in cyberspace and deny the same to our adversaries."[12] In other words, its mission is centered on integrating cyber initiatives of the military services to provide a holistic approach in securing cyberspace and combating threats. In combination with the NSA, it attempts to identify and exploit vulnerabilities of state and non-state adversary networks while defending our own. The Air Force is surely in line with this intent although there is significant room for improvement.

The mission of the U.S. Air Force is to "fly, fight and win…in air, space, and cyberspace."[13] On the surface, it appears the cyberspace mission is nothing more than a natural extension of the air and space domains. After all, there is an innate technology-related essence that the service has harnessed to apply airpower throughout its history. However, supporting cyberspace operations has often proven to be difficult and cumbersome endeavor since cyberspace as a

domain is relatively new and cyber doctrine is still being generated.

The Air Force has been very effective in dominating the air domain. In fact, there are very few nations in the world today that would pose a serious threat to the United States in air-to-air or air-to-ground scenario. Our aviators receive the most advanced aerial training year-round to ensure their competencies may be relied upon when needed. Furthermore, many senior Air Force leaders have traditionally been pilots at one point or another in their military careers.

The service has organized itself to support the space domain. That is, a major command (MAJCOM) for space-related issues has been established—Air Force Space Command (AFSPC)—which is the oldest MAJCOM in the Air Force.[14] The fact is that the integration of technological advances in space provides a monumental advantage to those nations in a position to exploit it. Therefore, it comes to no surprise that the Air Force has allocated personnel, training, doctrine and resources accordingly. After all, the use of satellite imagery and the Global Positioning System (GPS) in the preparation and execution phases of armed conflict is considered to be a beneficial asset in warfare. Once again, Air Force leaders understand this domain and its value.

Now look at the cyber domain. If one were to ask senior decision makers to define the cyber domain and explain how the Air Force has postured itself to combat cyber threats, chances are they would likely be unable to effectively do so—to no fault of their own. The simple fact is that cyberspace is so complex and overwhelming that it demands a drastic change in mindset.

Cyberspace is the only man-made domain and surpasses the boundaries associated with land, sea, air and space.[15] As a result, understanding the basic fundamentals in this operational environment requires more time and effort. It is also important to note that few senior leaders have had exposure to the cyber domain until late in their careers. This has translated into the

quandary in which we currently find ourselves: the need to improve intelligence support to cyberspace operations as a whole.

The Air Force's answer to the cyber domain problem is essentially the 24th Air Force. A large portion of its mission is to provide combatant commanders with trained cyber forces. It is also specifically charged with the establishment, operation and defense of Air Force networks as well as conducting the full range of cyber operations. [16] In other words, the 24th Air Force is the leading organization for cyberspace-related issues—and currently does not receive the vital intelligence support that it needs to be effective.

This over-arching organization is divided into three distinct agencies. These sub-divisions include the 67th Network Warfare Wing at Lackland AFB, Texas; the 688th Information Operations Wing at Lackland AFB, Texas; and the 689th Combat Communications Wing based out of Robbins AFB, Georgia. [17] Each of these is responsible for a section of the 24th Air Force mission—from defending Air Force networks to training personnel for full-spectrum operations, but do not appear to have an organic, robust intelligence support network as the Air Force is in the process of posturing itself to better support cyber operations from an Intel standpoint.

This may seem impressive on the surface. That is to say, it certainly appears there is a serious effort underway to ensure the forces provide to combatant commanders from the Air Force are organized, trained and equipped to an acceptable standard. However, it is making slow progress in a domain where speed is essential. This must be addressed before we fall further behind.

Cyberspace operations are conducted quickly. The speed in which cyberspace attacks take place emphasizes a significant need for timely and accurate intelligence support. After all, Intel knowledge of threats drives operations. Therefore, there is a requirement for quality Joint Intelligence Preparation of the Operational Environment (JIPOE) for senior decision makers and

operators, specifically relating to cyberspace.

A relatively new phrase to describe this type of support is *Cyber Intelligence, Surveillance, and Reconnaissance*, or cyber ISR. This term recognizes that successful attack and defense in the cyber domain require detailed knowledge of one's own capabilities and networks as well as those belonging to an adversary. [18] This goes beyond mapping computer systems and identifying specific technical characteristics. While this information is very useful, it is not the only piece of intelligence that may be derived. The fact is, Intel is an umbrella of information.

Air Force intelligence personnel must understand that tactics, techniques, and procedures (TTPs) and an adversary's intentions are equally important. In other words, the ways in which adversaries attempt to exploit our networks to gain an advantage (and the reasons why they do this) are within the purview of the intelligence realm. In this regard, intelligence is vital to provide an accurate picture of adversaries as well as their capabilities and limitations. It also assists in predicting the events that may occur in cyberspace. [19]

Interestingly enough, it is also important to note that intelligence operations themselves rely heavily on cyberspace. The Air Force has a term for this, Computer Network Exploitation (CNE), which is a subset of Signals Intelligence (SIGINT). As a major contributor to military operations, Intel leverages the cyber domain and exploits sensitive information. [20] The irony here is that intelligence professionals leverage cyberspace to exploit information and provide Intel to others, but lack the required training to understand how to support cyberspace attack and defense operations. Nonetheless, cyber doctrine is being published and intelligence training is being planned; such endeavors will assist in fixing this dilemma, but may fall short since Intel seems to be learning how to support Computer Network Attack (CNA) and Computer Network Defense (CND) operations.

Cyber Doctrine

There must be no ambiguity in terms of definition or classification when determining what constitutes a cyber threat, much less how to combat it. From an Intel standpoint, this means possessing a fundamental understanding of the cyber domain and being able to utilize the holistic approaches approved to combat cyberspace threats. After all, it is difficult to provide adequate support to these non-traditional operations if there is a lack of cyberspace awareness.

One of the primary methods for increasing awareness is to ensure cyber-related materials are made available. Doctrine, and other reference materials, must be published to avoid ambiguities associated with the cyber domain in order to provide a general guide on how one should ponder, plan and execute support for cyberspace operations; otherwise, Air Force Intel efforts will not be optimized for this domain. It is absolutely critical that these resources make it to the hands of those that need the information in order to maximize the chance of success against these non-conventional adversary threats.

In the past few years, there have been a number of documents created to assist in this regard. These range from the national level and are designed as a way that organizations at the lower echelons build their strategies. It is important to mention some of the more significant documents at the international, national and DOD levels to better understand the importance of setting our Air Force intelligence professionals up for success.

Earlier this year, the Obama Administration released and disseminated the *International Strategy for Cyberspace.* It is designed to reinforce the concept of strengthening partnerships in order to collectively address cyber threats. The idea is to combine efforts to secure cyberspace by dissuading cyber threats from "…terrorists, cybercriminals, or states and their proxies." [21]

The main focus of this publication is to collaborate with other states and build a united front

against such threats and is based on the latest version of the U.S. National Security Strategy (NSS). The 2010 NSS states that cyber poses a serious threat and highlights the manner in which these threats may infringe upon our national sovereignty. [22] As with the international strategy, this represents an acknowledgement by our most senior government officials that cybersecurity is a serious issue. After all, significant technological advances in recent years have allowed cyber threats to flourish. Both documents serve to underscore the significance of these threats.

At the DOD level, there are also several publications worthy of mention. The first of these publications are the National Defense Strategy (NDS) and the National Military Strategy (NMS) of the United States. Each of these documents echo much of the verbiage found in the NSS in highlighting the significance of cyberspace threats. Therefore, one may argue that securing the cyber domain is important…including countering the cyberspace-related objectives of violent extremists by deterring/defeating their aggression. [23]

Second, there is the 2011 *DOD Strategy for Operating in Cyberspace*. As the name suggests, it is an overall guide the Defense Department has approved for conducting operations in the cyber domain. It recognizes the that cybersecurity is a global issue by emphasizing the need for unity of effort within the DOD, leveraging the assistance of the interagency, and cooperating with international partners in order to "…mitigate the risks posed to U.S. and allied cyberspace capabilities." [24] These broad concepts act as guides to help refine those at the service level.

Finally, there is the Air Force service level primary publication. Entitled "Cyberspace Operations", Air Force Doctrine Document 3-12 (15 July 2010) is the latest guide for Airmen designed for Airmen to gather basic information regarding cyberspace operations. In this case, the Air Force underscores the importance of the outlining cyberspace fundamentals, command and organization of service cyber forces, as well as basic considerations for planning and

executing cyber missions. [25] This is a forward-leaning endeavor but is not all-inclusive.

While better late than never, these publications speak of intelligence support to cyberspace in general terms—but do not clarify exactly *how* the IC should provide support. The truth is that these documents must be detailed enough for intelligence personnel to reference when providing Intel support to cyberspace operations. After all, specific Intel-related documents are critical to leverage assistance in support of cyber.

Quite frankly, national-level documents and operational-level documents are being released fairly late in the game. This is not to suggest that they are useless since it is better late than never. However, it is fair to assert that it will take some time for organizations involved with combating cyber threats to streamline efforts based on the general principles outlined in these publications. Again, there is an abundance of vague information presented as to how intelligence personnel will be expected to support cyberspace operations.

These documents recognize the importance of information sharing. It also indicates that there should be cooperation among government agencies, the private sector, and multinational partners. However, there is very little information regarding the manner in which Intelligence personnel should conduct day-to-day operations against these threats.

The bottom line is cyber doctrine lacks specificity when speaking of providing intelligence support to cyberspace operations. This may be partly due to the fact that cyber is a relatively new and complex issue for intelligence professionals and decision makers to fully understand. In the Air Force, there appears to be significant progress made thus far but there is also quite a ways to go before its intelligence network properly supports this domain. In particular, there needs to be more progress made in terms of cyber training for intelligence professionals in the Air Force.

Intelligence Cyber Training

There is significant verbiage dedicated to the creation of professionals that understand the cyber domain across the board. The NSS in particular calls for a cadre of qualified personnel to secure cyberspace. [26] It also emphasizes the critical role cyberspace training plays.

The Air Force has made significant headway in reorganizing itself for cyberspace operations over the past few years. The creation of the 24th Air Force is an example of a shift in the right direction because it consolidates efforts across the service in support of cyber. In addition, there has been an effort to professionalize the officer cyber forces. The former establishes an official command and control structure; the latter provides opportunity for career progression in this unique field—particularly since it requires technical expertise.

By and large, many Air Force intelligence personnel and leaders currently do not understand the basics of cyber (to include specific capabilities and limitations). They also do not know who the "go-to guys" are for this domain. As a community, we fear what we do not understand and cyberspace seems to fall into that category. Emerging leaders on the officer side of the house in particular need to be familiar with the cyber domain and be exposed to cyberspace issues.

At the Air Force Command and Staff College (ACSC) at Maxwell AFB, cyberspace awareness and training is minimal to say the least. Statistically, these students represent the "top 20%" [27] of majors in their respective career fields and receive extremely limited exposure to cyber in the ACSC curriculum. The cyberspace elective, which accommodates 12-15 students per semester (of approximately 500 total students that attend ACSC each year), is the main forum available to students to dive deeper into this field of study. [28]

There are currently 20 Air Force Intelligence officers at ACSC during Academic Year 2012 (AY12). [29] Of these officers, the author of this research paper is the only one enrolled in the

cyber elective during the fall semester. Unless any of these officers enroll in the cyber elective during the spring semester at ACSC, there may only be one Air Force Intel officer coming out of ACSC this year with any refined understanding of cyberspace operations.

Given this situation, it appears that many future Air Force leaders will continue failing to understand the importance of cyberspace. The ramifications of this are serious: since students completing ACSC in-residence will theoretically become commanders and staff officers in the future, they are not set up for success if faced with a challenging cyberspace-related issue in their future jobs. In addition, ACSC has not focused on Intelligence, Surveillance and Reconnaissance (ISR) education. This means those cyberspace officers in the 17D career field are not be clear on the capabilities that Intel personnel provide in support of their efforts.

Nor does the Air Force have an adequate amount of thoroughly trained personnel to provide the level of specialized intelligence support needed to plan and conduct operations against cyber threats. USCYBERCOM is a step in the right direction for DOD and the 24th Air Force is on point to support accordingly. However, the Air Force must provide training during Intel-specific Professional Military Education (PME) in order for its intelligence personnel to adequately support cyberspace operations.

The Air Force Intelligence Officer Course at Goodfellow Air Force Base provides a solid example of this dilemma. As of December 2011, there is an absence of cyber training for new second lieutenants entering the Intel career field. In fact, the current curriculum does not dedicate any training hours to cyberspace operations. [30] This means new Intel officers may find themselves in assignments in which they will be asked to support cyberspace without any formal training at the present time.

It is important to note that the Air Force Intel leadership is working on this problem. The

315th Training Squadron in particular, which develops new Air Force Intelligence Officers each year, has made the effort to produce better-qualified, cyber aware Intel officers in future courses. They recognize the growing need for intelligence support to cyberspace operations and are attempting to fix this delta. That is, the Air Force Intelligence Officer Course is being revamped to integrate 12 hours of cyber in conjunction with 12 hours of space as part of the same instructional block. [31] Presumably, this will include basic cyber fundamentals into the curriculum so that new Intel officers do not show up at a unit without any knowledge of what cyber is, much less how to support it from an Intel perspective.

Air Force Intel professionals must comprehend the complexities involved in cyberspace. After all, the Department of Defense has reported to Congress in Nov 2011 that it "strives to secure the best possible intelligence about potential adversaries' cyber capabilities." [32] This implies that Intel professionals have been trained to conduct this type of activity. If we are not able to discern what cyberspace is, how can we possibly posture ourselves to support operations in this domain? Therefore, it is important to emphasize the training aspect for the Air Force intelligence community regarding cyberspace operations since a lot is being learned on the job.

Learning on the job is a temporary solution for the larger issue of creating cyber-savvy Intel personnel. As discussed later, the Air Force is making some advancement in this arena but it requires a jump-start of sorts to gain momentum. While this concern is likely recognized as a necessity across the board, it will take a lengthy period since the cyber domain is relatively new. Nonetheless, there are a few initiatives coming online to bring intelligence professionals closer to realistically providing sensitive information that may be of use to thwart cyberspace dangers.

This is not to say Air Force Intel is lagging too far behind. However, we must expedite the process. We simply cannot wait any longer; we must strive to raise cyber awareness within our

career field immediately—senior leaders as well as the rank and file—to avoid a grave situation in which Air Force intelligence is desperately needed in an operation and is unable to provide the adequate level of support. The worst-case scenario is the dreaded cyberspace equivalent of 9/11.

The good news is that there is an effort underway by the Air Force to address this problem. In fact, the Air Force Cyber ISR Force Development Roadmap (currently in draft) outlines plans for such critical issues as training intelligence personnel in support of cyberspace operations and the developing officer as well as enlisted personnel from a career path perspective. [33] This is a clear indication that the Air Force has taken this issue seriously and is making plans to correct this deficiency in an effort to organize, train and equip intelligence professionals in a manner that best suits the Air Force in support of cyberspace operations.

Thus, in terms of intelligence cyber training, there needs to be more done. The NSS specifies the importance of information gathering and sharing in support of cyberspace operations. While there are multiple efforts underway, the Air Force in particular must continue to quickly tackle this issue. After all, cyberspace operations are in need of timely and accurate Intel support.

Recommendations

The Air Force has not optimized its intelligence support to cyberspace operations. It is likely because cyberspace requires a different method of thinking as a result of the complex nature of this domain. However, there are several ways in which the Air Force may improve this dilemma. Although they will prove to be challenging at the onset, the following suggestions will serve to benefit the Air Force intelligence community. They are based on research conducted in 2011.

First and foremost, there must be a mindset change. Senior leaders must stress the importance of cyberspace at the highest levels. This means taking the time to comprehend basic principles and wholeheartedly accepting the notion that our adversaries pose a serious threat by attempting to exploit us daily. Cyber threats will not go away; they will only increase in frequency and sophistication over time. It is precisely for this reason that Air Force Intel must adapt fast.

This is not to say that the mindset change is limited to senior leaders. However, these issues must be addressed at the top of the Air Force hierarchy if they are to gain traction. One way to do this would be to synchronize PME with cyberspace. For instance, the Air Force may include initiatives to strengthen the Air Force Intelligence Officer Course to teach basic cyberspace fundamentals and the ACSC curriculum for future Air Force commanders and staff officers by integrating cyberspace planning.

Simply put, Air Force leadership must foster an environment in which non-kinetic operations are afforded as much attention as traditional, kinetic operations. This includes the establishment (and enforcement) of policies aimed at improving intelligence support to cyberspace operations. The Air Force has been confortable in the kinetic world for decades; it is now time to mentally embrace the cyber domain in order to better understand and support it.

There simply must be a top-down approach since the greatest change will occur when Airmen

see that their leadership is on-board, leading by example to confront the cyberspace problem. This means major Air Force exercises such as Red Flag, Blue Flag, and Green Flag evolutions must contain elements of cyberspace operations. By doing so, attendees would be exposed to cyber threats and be in a position to plan against them—including Intel support in this domain.

Second, Air Force doctrine must quickly catch up to address cyber threats. There are multiple documents that have recently been published at the national and operational levels. However, Air Force intelligence personnel require the ability to reference service publications regarding the support of cyberspace operations. These documents would serve as a general guide on the various issues that should be considered in the operational environment specific to cyberspace.

While Air Force Doctrine Document 3-12 does provide general information, there must be further efforts to streamline the manner in which the Air Force supports operational counterparts in cyber as we do in other domains. We need to make an impact if we claim to be the service that leads cyberspace as indicated in the Air Force mission statement. After all, doctrine lacks focus on *how* to support the cyber domain, which is required by Intel professionals charged with supporting cyber efforts.

Finally, the Air Force must build a cadre of cyber-savvy intelligence personnel to better assist in combating cyber threats. By doing so, the Air Force will be in compliance with the notion that "the Intelligence Community and U.S. Cyber Command continue to develop a highly skilled cadre of (cyberspace) forensic experts." [34] This means heavy emphasis must be placed on the creation of a pool from which cyber-savvy intelligence professionals are drawn, guaranteeing career progress opportunities to ensure skillsets are not lost. Currently, there is an insufficient amount of cyber-trained personnel to leverage this assistance from.

Conclusion

The recent creation of cyber as a domain is a direct reflection of the importance placed on it by senior officials. Quite frankly, cyberspace has become the latest manner in which adversaries infringe upon the sovereignty of the United States. After all, unlike the other domains that have physical borders, there are special characteristics inherent to cyberspace—making it complex.

Despite its significance, the Air Force is making slow progress in posturing itself to deal with cyber threats in an era marked by rapid technology change. This is probably due to the lack of a mindset change from the senior echelons of Air Force leadership. They must advocate cyber at their level and reinforce the significance of cyberspace operations in leading by example.

The service has created the 24th Air Force as a way to consolidate its efforts in cyberspace, which is certainly a giant step in the right direction. Although its mission should be refined to better assist USCYBERCOM, it has made progress from a command and control perspective in particular. There is no question that cyber warriors are headed on a good path.

There is still some work that needs to be done in terms of intelligence support to cyberspace operations. In addition to the mindset change mentioned above, cyber doctrine and training are two areas lacking attention. While there are several efforts underway to remedy this problem, it will take some time before it reaches fruition.

In the end, there must be a concerted top-down, leadership approach to improving U.S. Air Force intelligence support to cyberspace operations. While progress has been made in the fairly recent past, there are a few issues that should be resolved before the Air Force may adequately assist operational counterparts focused on the cyber domain. This paper identified the importance of the cyber domain, the necessary mindset change within the Air Force, and offered recommendations on how to better posture Air Force Intel posture combat cyber threats.

Endnotes

[1] Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. National Defense University Press: Washington DC, 2009, Pp. 314-315
[2] Richelson, Jeffrey T. *The US Intelligence Community*. 2008, Boulder, Colorado: Westview Press, Pp. 2-3
[3] Ibid, 12
[4] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*. Official Government Edition, Washington DC: US Government Printing Office, 2004, Pp. 1-13
[5] Ibid, 416-417
[6] Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. National Defense University Press: Washington DC, 2009, Pp. 177-178
[7] Ibid, 466-469
[8] Richelson, Jeffrey T. *The US Intelligence Community*. 2008, Boulder, Colorado: Westview Press, Pp. 16
[9] Office of the Director of National Intelligence, http://www.dni.gov/faq_intel.htm (accessed 09 October 2011)
[10] Odom, William E. *Fixing Intelligence for a More Secure America*. 2004, New Haven, Connecticut: Yale University Press, Pp. 185
[11] Ibid, 115-117
[12] U.S. Department of Defense, Cyber Command Fact Sheet, 21 May 2010 http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed 10 November 2011)
[13] Convertino, Sebastian M., Lou Anne DeMattei and Tammy M. Knierim. *Flying and Fighting in Cyberspace*. Air University: Air University Press, 2007, Pp.1
[14] United States Air Force. "Major Commands." USAF Almanac, 2010. http://www.airforcemagazine.com/MagazineArchive/Magazine%20Documents/2010/May%2020 10/0510majcoms.pdf (accessed 13 December 2011)
[15] Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009, Pp. 11
[16] U.S. Department of Defense, 24th Air Force Fact Sheet, 01 April 2010. http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663 (accessed 20 Nov 2011)
[17] Ibid
[18] Convertino, Sebastian M., Lou Anne DeMattei and Tammy M. Knierim. *Flying and Fighting in Cyberspace*. Air University: Air University Press, 2007, Pp. 44-49
[19] Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press: RAND, 2007, Pp. 90-92
[20] Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. National Defense University Press: Washington DC, 2009, Pp. 293
[21] *International Strategy for Cyberspace*. Washington DC: The White House, May 2011, Pp.12
[22] *National Security Strategy of the United States of America.* Washington DC: The White House, May 2010, Pp. 27-28
[23] *National Military Strategy of the United States of America*. Washington DC: Department of Defense, February 2011, Pp. 3-7
[24] *Department of Defense Strategy for Operating in Cyberspace*. Washington DC: Department of Defense, July 2011, Pp. 1-3

[25] Air Force Doctrine Document 3-12. *Cyberspace Operations*. , 2010, Pp. 1-30
[26] *National Security Strategy of the United States of America.* Washington DC: The White House, May 2010, Pp. 27
[27] Maj Todd R. Lancaster. "Air Force Mentoring: Developing Leaders." Air Command and Staff College: Air University, 2003. Pp. 16
http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA424958 (accessed 13 December 2011)
[28] Lt Col John Matus, untitled lecture, Air Command and Staff College, Maxwell AFB, AL, 19 October 2011.
[29] Maj James Hall, Air Force Intelligence Officer and student, Air Command and Staff College, Maxwell AFB, AL, to the author, email, 05 December 2011.
[30] Maj Charles Woods, Intelligence Officer Course Flight Commander, 315th Training Squadron, Goodfellow AFB, TX, to the author, email, 06 December 2011.
[31] Ibid
[32] Department of Defense. *United States Cyber Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 2011, Pp. 3
[33] Department of the Air Force, A2. "Air Force Cyber Intelligence, Surveillance, and Reconnaissance Development Roadmap." Draft, 2011, Pp. 3-15
[34] Department of Defense. *United States Cyber Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 2011, Pp. 4

Bibliography

Convertino, Sebastian M., Lou Anne DeMattei and Tammy M. Knierim. *Flying and Fighting in Cyberspace*. Air University: Air University Press, 2007

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington DC: Department of Defense, July 2011

Department of Defense. *United States Cyber Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 2011

Department of the Air Force, A2. "Air Force Cyber Intelligence, Surveillance, and Reconnaissance Development Roadmap." Draft, 2011

Hall, Maj James, Air Force Intelligence Officer and student, Air Command and Staff College, Maxwell AFB, AL. To the author. E-mail, 05 December 2011.

International Strategy for Cyberspace. Washington DC: The White House, May 2011

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. National Defense University Press: Washington DC, 2009

Lancaster, Maj Todd R. "Air Force Mentoring: Developing Leaders." Air Command and Staff College: Air University, 2003.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press: RAND, 2007

National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*. Government Edition, Washington DC: US Government Printing Office, 2004.

National Military Strategy of the United States of America. Washington DC: Department of Defense, February 2011

National Security Strategy of the United States of America. Washington DC: The White House, May 2010

Odom, William E. *Fixing Intelligence for a More Secure America*. New Haven, Connecticut: Yale University Press, 2004

Richelson, Jeffrey T. *The US Intelligence Community*. 2008, Boulder, Colorado: Westview Press

United States Air Force. "Major Commands." USAF Almanac, 2010.

U.S. Department of Defense, 24th Air Force Fact Sheet, 01 April 2010

http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663 (accessed 20 Nov 2011)

U.S. Department of Defense, Cyber Command Fact Sheet, 21 May 2010 http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed 20 Nov 2011)

Woods, Maj Charles, Intelligence Officer Course Flight Commander, 315th Training Squadron, Goodfellow AFB, TX. To the author. Email, 06 December 2011.